IN THE CLAIMS

Please amend the claims as follows:

1. (Currently amended) A method for filtering out exploits passing through a device, comprising:

receiving an object directed to the device;

determining a first hash value associated with the object;

determining a second set of hash values associated with objects that have previously been scanned;

if the first hash value matches at least one of the hash values in the second set,

determining a third hash value associated with the object;

determining a fourth set of hash values associated with the objects that have previously been scanned; and

if the third hash value matches at least one of the hash values in the fourth set, immediately processing the object.

2. (Canceled)

3. (Canceled)

4. (Currently amended) The method of Claim 1, wherein the first hash value includes a rough outline hash value (ROHV).

5. (Currently amended) The method of Claim 4, wherein the third hash value includes a sophisticated signature hash value (SSHV) and wherein the ROHV requires less time to compute than the SSHV.

6. (Currently amended) The method of Claim 1, wherein immediately processing the object further comprises ~~processing~~ forwarding the object to an output component without scanning the object.

7. (Canceled)

8. (Original) The method of Claim 6, wherein immediately processing the object further comprises forwarding the object to a destination.

9. (Currently amended) The method of Claim 1, further comprising if the first hash value does not match any of the hash values in the second set,

scanning the object for an exploit; and

updating the second set of hash values to include the first hash value.

10. (Currently amended) The method of Claim 1, further comprising if the third hash value does not match any of the hash values in the fourth set,

scanning the object for an exploit; and

updating the fourth set of hash values to include the third hash value.

11. (Canceled)

12. (Currently Amended) A computer-readable medium encoded with a data-structure, comprising:

a first indexing data field having indexing entries, each indexing entry including a first hash value; and

a second data field including object-related entries, each object-related entry having a second hash value and being indexed to an indexing entry in the first indexing data field, each object-related entry being uniquely associated with an object that has been previously scanned.

13. (Canceled)

14. (Currently amended) The computer-readable medium of Claim 12, wherein the first hash value is a rough outline hash value (ROHV) [ROHV].

15 (Currently amended) The computer-readable medium of Claim 12, wherein the second hash value is a sophisticated signature hash value (SSHV) [SSHV].

16. (Original) The computer-readable medium of Claim 12, wherein at least one object-related entry in the second data field includes information about the associated object.

17. (Original) A system for protecting a device against an exploit, comprising:

a message tracker that is configured to determine whether an object has been previously scanned using a two-phase hash value technique; and

a scanner component that is coupled to the message tracker and that is configured to receive an unscanned object and to determine whether the unscanned object includes an exploit.

18. (Canceled)

19. (Currently amended) The system of Claim 17, wherein the two-phase hash value technique comprises:

determining a first hash value associated with the object;

determining a second set of hash values associated with objects that have previously been scanned; and

if the first hash value does not match at least one of the hash values in the second set, determining that the object has not been previously scanned.

20. (Canceled)

21. (Currently amended) The system of Claim 19, wherein the first hash value further comprises a ROHV.

22. (Currently amended) The system of claim 19, wherein the two-phase hash value technique further comprises:

if the first hash value matches at least one of the hash values in the second set,

determining a third hash value associated with the object;

determining a fourth set of hash values associated with the objects that have previously been scanned;

if the third hash value does not match at least one of the hash values in the fourth set, determining that the object has not been previously scanned.

23. (Canceled)

24. (Currently amended) The system of Claim 22, wherein the third hash value further comprises a SSHV.

25. (Currently amended) The system of Claim 22, wherein the two-phase hash value technique further comprises:

if the third hash value approximately matches at least one of the hash values in the fourth set, determining that the object has been previously scanned.

26-29. (Canceled)

30. (New): The method of Claim 1, wherein:

the first hash value and hash second value are determined by the device; and

the second set of hash values and the fourth set of hash values are determined by the device based on previous scanning by the device.

31. (New): The method of claim 1, wherein the method is performed by a firewall.

32. (New): The method of claim 1, wherein the method is performed by a router.

33. (New): The method of claim 1, further comprising:

determining whether the object is compressed; and

if the object is compressed, decompressing the object.

34. (New): The system of claim 17, wherein the system includes a firewall.

35. (New): The system of claim 17, wherein the system includes a router.

36. (New): A method comprising:

receiving an object;

matching a rough outline hash value (ROHV) of the object to ROHVs of known objects;

if a match is found between the ROHV of the object to any of the ROHVs of the known objects, matching a sophisticated signature hash value (SSHV) of the objects to SSHVs of the known objects;

if a match is found between the SSHV of the object to any of the SSHVs of the known objects, processing the object as a malicious object;

if a match is not found between either the ROHV of the object to any of the ROHVs of the known objects or the SSHV of the object to any of the SSHVs of the known objects, scanning the object; and

if the scanning the object determines that the object is malicious, processing the object as a malicious object and updating the ROHVs of known objects and the SSHVs of the known objects.